How can ANALYTICS improve your CYBER SECURITY?

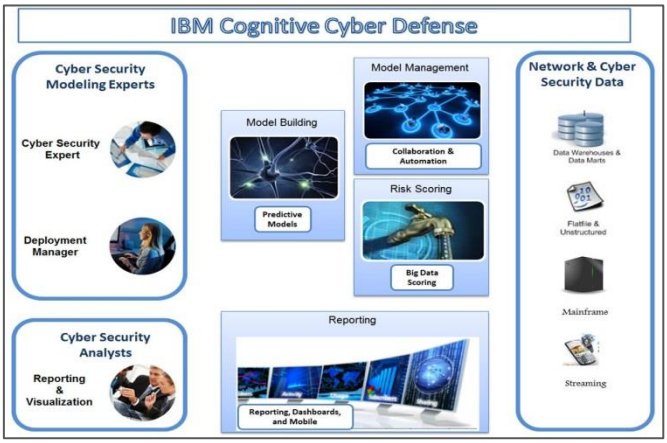

Figure 1: Cyber Security Defense Architecture

Computer-based intrusions against U.S. infrastructure have increased over 48% in 2014. Over one trillion dollars of US intellectual property have been stolen in these attacks.

Most currently-available cyber security tools and solutions use rule and signature –based analyses to detect threats. Jeskell's **CyberSentinel™ Threat Detector** employs a new tactic: the use of ***machine learning models*** to identify threats *as they occur* in real-time.

These machine learning analytics, along with dynamic decision modeling, can predict, identify, and disrupt Advanced Persistent Threats (APT) *in real-time,* providing more comprehensive security. Diagnostic analytics and activity alerts allow security professionals to perform deep forensic and drill-down analysis of detected threats.

CyberSentinel is pre-integrated and pre-configured with proven, state-of-the-art machine learning models from IBM Research, with the ability to build new families of cyber models to react to the ever-changing APT environment. It is also designed to complement and extend popular Security and Information Management (SIEM), Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS).

CyberSentinel does not replace these traditional rule and signature based systems; it works with them to catch what other tools miss. In addition, standard responses can be enabled to automatically respond to identified threats.

CyberSentinel ships with a core set of pre-tested machine learning cyber models that perform DNS behavior modeling, as well as specific DNS related attack types. These models are designed to adapt to the specific patterns in your data, and to the nature of the threats you are trying to detect. Additionally, **CyberSentinel** includes IBM's industry leading Predictive Modeling Workbench, allowing customers to design and deploy new cyber models.

Solution Components

IBM Analytic and Big Data technologies form the core of **CyberSentinel**. These market-leading and mature technologies are designed to enable security specialists to conduct proactive network defense with a system that is optimized for cyber security. It is designed, tuned, and configured to address the complex threat environment. For example, **CyberSentinel** features the following components:

- ***Modeling Framework*** *based on SPSS Modeler 16 and InfoSphere Streams SPSS Analytics Toolkit for the creation of new-custom models, including:* Time series, Regression, Clustering, Association, *& more*

Figure 2: IBM QRadar Dashboard

- ***Machine Based Learning Models*** *for Cyber, including:* Fast Fluxing, Beaconing and Exfiltration detection, DNS Tunneling, Domain Generation Algorithm (DGA) Detection, DNS Amplification, and Deep Packet Inspection via InfoSphere Streams Protocol Analysis Module (PAM)

- ***Big Data Analytics Interoperability*** *with many of the popular big data repository and Cyber solutions, including:* IBM InfoSphere BigInsights, IBM QRadar, Cloudera, Hortonworks, Accumulo, Mongo DB, Splunk/Hunk, and HPArc Sight

- ***Rich toolset*** *to provide ease of use and advanced streaming computing environment to conduct true real time analysis on data in motion, such as*: Predictive Analytics, Data Mining, and a Streaming Analysis Environment; Advanced Visualization and Diagnostic Analytics within the cyber cockpit via Cognos BI with interfaces to Google Maps; Model management ability to build new models and refine existing models based on changing threats; and a Framework whereby models can dynamically update based on changing threat vectors

"An ever-changing and increasingly sophisticated cyber threat environment requires an equally adaptive and innovative defense"

Solution Capabilities

CyberSentinel enables users to better understand the threat landscape, spot anomalies across network traffic, and compare and compile reports across activities or threat vectors. Its core capabilities are made up of the following:

Machine Learning Models

These predictive models provide insight into hidden patterns and enable the organization to anticipate change within their cyber security threat landscape and identify threats as they occur. The heart of **CyberSentinel** is SPSS Modeler 17 Gold and InfoSphere Streams with adapters to a variety of SIEM solutions, Visualization, Hadoop Cloud and other data repositories. Models built with R, MatLab or SPSS can be imported into InfoSphere streams for inclusion into the base family of cyber models.

Built within IBM's industry-leading predictive analytics workbench, these models can be automatically tuned to each agency's data environment. This optimizes the models to the specific nuances of each organization's cyber mission and data landscape.

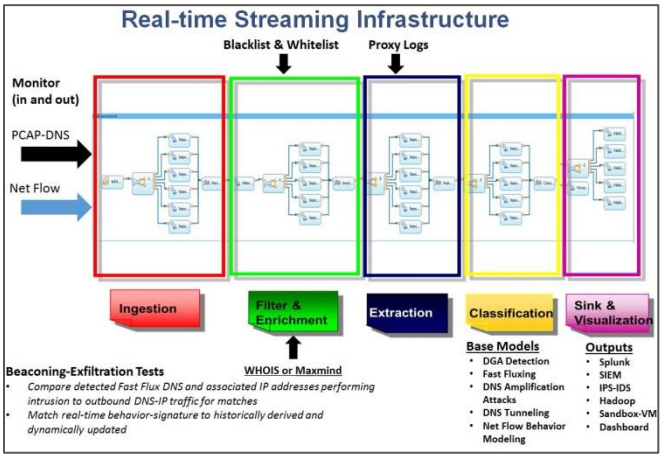

Figure 3: CyberSentinel real-time streaming architecture

The workbench is a flexible, comprehensive data mining tool with a highly intuitive visual interface, enabling trained users to quickly modify existing models and develop new models. The workbench supports the entire predictive analytics process from data access and preparation, to visualization and discovery analysis, and can export results into a database or application. The solution includes the option for each model to automatically monitor its performance and adapt to new incoming data.

Network Behavior Monitoring & Visualization

This solution includes pre-trained Behavior Models for DNS Traffic analysis as well as the necessary software and pre-configured connections to automatically deploy cyber security predictive models to a streaming environment for real time risk detection across your network traffic. Once a predictive model has been built, tested, and validated it is made available via the included analytical asset repository. Using this repository, models can be activated to monitor network data and provide risk scores relative to known or unusual patterns. The **CyberSentinel** solution also integrates with the pre-built visualization tools you already have (e.g. Microsoft Excel) to provide enterprise class cyber intelligence specifically tuned for the Advanced Persistent Threat (APT) environment.

To learn more, visit us on the web at www.jeskell.com, or scan our QR Code on the left.

CyberSentinel by Jeskell Systems

Premier Business Partner IBM